附件2



**吉林大学重要信息系统**

**安全专项检查自查表**

单位名称 （加盖单位公章）

自查时间

|  |
| --- |
| 一、单位基本情况 |
| 信息安全工作管理部门负责人 | 姓名 |  | 职务/职称 |  |
| 办公电话 |  | 移动电话 |  |
| 信息安全技术责任部门联系人 | 姓名 |  | 职务/职称 |  |
| 办公电话 |  | 移动电话 |  |
| 二、 信息安全工作情况 |
| 1. 信息安全协调（领导）机构的建立和运行情况 |
| （包括机构建立、组成、主要职责以及信息安全工作议事或例会制度等具体情况） |
| 2. 信息安全责任制落实情况 |
| （包括安全责任分工、信息系统安全责任人、签订信息安全责任书及责任追究制度落实等具体情况） |
| 3. 信息安全规划、策略制定和落实情况 |
| （包括信息安全工作的短期目标和长远规划、网络安全策略制定和执行、网络安全工作在信息化建设工作落实情况，如同步立项、同步设计、同步建设、同步验收、同步运维等） |
| 4. 信息安全工作组织保障和考核情况 |
| （包括定期召开信息安全工作会议或印发文件部署网络安全工作，信息安全工作考核纳入到年度考核指标、信息安全工作的经费预算等情况） |
| 5. 信息安全人员管理制度建立和执行情况 |
| （包括人员录用、安全培训、技术考核、安全保密、人员离岗等情况，其中安全培训包括本年度接受信息安全教育培训的人数、本年度获得“教育信息安全等级保护专业培训（管理类）合格证书”的人数、本年度获得“教育信息安全等级保护专业培训（技术类）合格证书”的人数。） |
| 6. 信息系统建设管理制度落实情况 |
| （包括在信息系统建设过程中产品采购、服务外包签订安全保密责任书、信息系统投入使用前进行安全性测试等有关情况） |

|  |
| --- |
| 7. 信息系统定级备案、等级测评和安全建设整改工作开展情况 |
| 序号 | 系统名称 | 定级备案 | 建设整改 | 等级测评 |
| 是否定级 | 所定级别 | 是否备案 | 是否整改 | 整改服务机构 | 是否测评 | 等级测评机构 |
| 1 |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |

|  |
| --- |
| 8. 信息系统基本情况 |
| 序号 | 系统名称 | 服务对象 | 联网情况 | 数据集中情况 | 灾备情况 | 业务连续性情况 | 开发模式 |
| 1 |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |
| **说明：**1. 表格中每个系统的“服务对象”“联网情况”“数据集中情况”“灾备情况”“业务连续性情况”“开发模式”请按照本说明内容填写对应项字母。
2. **服务对象：A** 面向社会 **B** 不面向社会
3. **联网情况：A** 可通过互联网直接访问 **B** 与互联网逻辑隔离 **C** 与互联网物理隔离
4. **数据集中情况：A** 全国集中 **B** 省级集中 **C** 不集中
5. **灾备情况：A** 系统级灾备 **B** 仅数据灾备 **C** 无灾备
6. **业务连续性情况：A** 可容忍中断时间小于30分钟 **B** 可容忍中断时间大于30分钟小于12小时 **C** 可容忍中断时间大于12小时

**开发模式：A** 自主设计开发（不含二次开发） **B** 国内厂商开发 **C** 国外厂商开发 **Ｄ** 采购国内厂商 **E** 采购国外厂商 |

|  |
| --- |
| 9. 信息安全监测预警及安全事件应急处置情况 |
| （包括信息安全日常监测预警机制的建立和落实，应急预案制定、应急保障技术支撑队伍的组织、定期应急演练，信息安全事件发生与处置等情况） |
| 10. 安全检查工作开展情况 |
| （包括安全检查工作的计划、部署、要求、方案实施、总结汇报、安全威胁发现和安全隐患整改等情况） |
| 11. 信息系统安全保护技术落实情况 |
| （包括机房、网络、主机、应用、数据等各方面的安全措施，如安全技术管理、监控报警、防攻击、防篡改、防泄漏及容灾备份等情况） |
| 12．信息系统使用国外信息技术产品和服务情况 |
|  | 操作系统 | 数据库 | 办公软件 | 服务器 | 路由器 | 交换机 | 磁盘阵列 | 磁带库 |
| 国内品牌数量（台/套） |  |  |  |  |  |  |  |  |
| 国外品牌数量（台/套） |  |  |  |  |  |  |  |  |
| 13．信息系统安全技术检测情况 |
| 恶意代码检测 | ①进行过病毒木马等恶意代码检测的服务器台数：\_\_\_\_\_\_\_\_\_\_\_其中，存在恶意代码的服务器台数：\_\_\_\_\_\_\_\_\_\_\_②进行过病毒木马等恶意代码检测的终端计算机台数：\_\_\_\_\_\_\_\_\_其中，存在恶意代码的终端计算机台数：\_\_\_\_\_\_\_\_\_\_\_ |
| 安全漏洞扫描 | ①进行过漏洞扫描的服务器台数：\_\_\_\_\_\_\_\_\_\_\_其中，存在漏洞的服务器台数：\_\_\_\_\_\_\_\_\_\_\_存在高风险漏洞的服务器台数：\_\_\_\_\_\_\_\_\_\_\_②进行过漏洞扫描的终端计算机台数：\_\_\_\_\_\_\_\_\_\_\_其中，存在漏洞的终端计算机台数：\_\_\_\_\_\_\_\_\_\_\_存在高风险漏洞的终端计算机台数：\_\_\_\_\_\_\_\_\_\_\_ |
| 源代码安全审计 | ①进行过源代码安全审计的系统数量：\_\_\_\_\_\_\_\_\_\_\_ |
| 渗透测试 | ①进行过安全渗透测试的系统数量：\_\_\_\_\_\_\_\_\_\_\_ |